

DEPARTMENT OF DEFENSE CONTRACT SECURITY CLASSIFICATION SPECIFICATION <i>(The requirements of the DoD Industrial Security Manual apply to all security aspects of this effort.)</i>				1. CLEARANCE AND SAFEGUARDING a. Facility Clearance Required YES b. Level of Safeguarding Required TS//SCI	
2. THIS SPECIFICATION IS FOR: (X and complete as applicable) <input type="checkbox"/> a. Prime Contract Number 1406-04-06-RP-44943 <input type="checkbox"/> b. Subcontract Number <input type="checkbox"/> c. Solicitation or Other Number Due Date (YYMMDD)			3. THIS SPECIFICATION IS: (X and complete as applicable) X a. Original (Complete date in all cases) Date (YYMMDD) <input type="checkbox"/> b. Revised (Supersedes all previous specs) Revision No. Date (YYMMDD) <input type="checkbox"/> c. Final (Complete Item 5 in all cases) Date (YYMMDD)		
4. IS THIS A FOLLOW-ON CONTRACT? <input type="checkbox"/> Yes X No. If YES, complete the following: Classified material received or generated under: _____ (Preceding Contract Number) is transferred to this follow-on contract.					
5. IS THIS A FINAL DD FORM 254? <input type="checkbox"/> Yes X No. If YES, complete the following: In response to the contractor's request dated _____, retention of the identified classified material is authorized for the period of _____.					
6. CONTRACTOR (Include Commercial and Government Entity (CAGE) Code)					
a. Name, Address, and Zip Code		B. CAGE Code		c. Cognizant Security Office (Name, Address, and Zip Code) Office of Security NSSO Program Security Office 14675 Lee Road Chantilly, VA, 20151-1715	
7. SUBCONTRACTOR					
a. Name, Address, and Zip Code		b. CAGE Code		c. Cognizant Security Office (Name, Address, and Zip Code)	
8. ACTUAL PERFORMANCE					
a. Location NSSO – Waples Mill, Pentagon, NRO and TASC (At all our geographically separate locations) and areas designated by the government in the D.C. Metro Area		b. CAGE Code		c. Cognizant Security Office (Name, Address, and Zip Code) same as 6c. above	
9. GENERAL IDENTIFICATION OF THIS PROCUREMENT The scope of this SOW encompasses the functions necessary to provide decision support throughout the lifecycle including the policy, strategy, planning, acquisition, and operational phases. Additionally, the contractor will provide the expertise to support the NSSO in its mission including evaluating and analyzing emerging needs and solutions.					
10. CONTRACTOR WILL REQUIRE ACCESS TO:			11. IN PERFORMING THIS CONTRACT, THE CONTRACTOR WILL:		
	YES	NO		YES	NO
a. Communications Security (COMSEC) Information	<input type="checkbox"/>	<input checked="" type="checkbox"/>	a. Have access to classified information only at another contractor's facility or a government activity	<input type="checkbox"/>	<input checked="" type="checkbox"/>
b. Restricted Data	<input type="checkbox"/>	<input checked="" type="checkbox"/>	b. Receive classified documents only	<input type="checkbox"/>	<input checked="" type="checkbox"/>
c. Critical Nuclear Weapon Design Information	<input type="checkbox"/>	<input checked="" type="checkbox"/>	c. Receive and generate classified material	<input checked="" type="checkbox"/>	<input type="checkbox"/>
d. Formerly Restricted Data	<input type="checkbox"/>	<input checked="" type="checkbox"/>	d. Fabricate, modify, or store classified hardware	<input type="checkbox"/>	<input checked="" type="checkbox"/>
e. Intelligence Information:			e. Perform services only	<input type="checkbox"/>	<input checked="" type="checkbox"/>
(1) Sensitive Compartmented Information (SCI)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	f. Have access to U.S. classified information outside the U.S., Puerto Rico, U.S. Possessions and Trust Territories	<input type="checkbox"/>	<input checked="" type="checkbox"/>
(2) Non-SCI	<input checked="" type="checkbox"/>	<input type="checkbox"/>	g. Be authorized to use the services of Defense Technical Information Center (DTIC) or other secondary distribution center	<input checked="" type="checkbox"/>	<input type="checkbox"/>
f. Special Access Information	<input type="checkbox"/>	<input checked="" type="checkbox"/>	h. Require a COMSEC account	<input type="checkbox"/>	<input checked="" type="checkbox"/>
g. NATO Information	<input type="checkbox"/>	<input checked="" type="checkbox"/>	i. Have TEMPEST requirements	<input checked="" type="checkbox"/>	<input type="checkbox"/>
h. Foreign Government Information	<input type="checkbox"/>	<input checked="" type="checkbox"/>	j. Have operations security (OPSEC) requirements	<input type="checkbox"/>	<input checked="" type="checkbox"/>
i. Limited Dissemination Information	<input type="checkbox"/>	<input checked="" type="checkbox"/>	k. Be authorized to use the Defense Courier Service	<input checked="" type="checkbox"/>	<input type="checkbox"/>
j. For Official Use Only Information	<input checked="" type="checkbox"/>	<input type="checkbox"/>	l. Other (Specify)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
k. Other (Specify)	<input type="checkbox"/>	<input checked="" type="checkbox"/>			

CL By:
CL Reason:
DECL On:
DRV From:

Attachment _____
To Contract _____

UNCLASSIFIED

12. PUBLIC RELEASE. Any information (*classified or unclassified*) pertaining to this contract shall not be released for public dissemination except as provided by the *Industrial Security Manual* or unless it has been approved for public release by appropriate U.S. Government authority. Proposed public releases shall be submitted for approval prior to release ☐ Direct ☒ Through (*Specify*)
to the Directorate for Freedom of Information and Security Review, Office of the Assistant Secretary of Defense (Public Affairs) for review. In the case of Non-DoD User Agencies, requests for disclosure shall be submitted to that agency.

13. SECURITY GUIDANCE. The security classification guidance needed for this classified effort is identified below. If any difficulty is encountered in applying this guidance or if any other contributing factor indicates a need for changes in this guidance, the contractor is authorized and encouraged to provide recommended changes; to challenge the guidance or the classification assigned to any information or material furnished or generated under this contract; and to submit any questions for interpretation of this guidance to the official identified below. Pending final decision, the information involved shall be handled and protected at the highest level of classification assigned or recommended. (*Fill in as appropriate for the classified effort. Attach, or forward under separate correspondence, any documents/guides/extracts referenced herein. Add additional pages as needed to provide complete guidance.*)

The security requirements and public release clause conveyed by this DD Form 254 apply only to classified information and activities conducted in the performance of the contract. "Reference Item 1a and 1b: NAM CLAUSE N52.204-001 and NAM CLAUSE N52.204-002 applies."

The contractor shall maintain an overall security program in accordance with the requirements of the NRO Classification Guide, the NRO Security Manual, other applicable SAP and program classification guides, program security guides, Director of Central Intelligence Directives (DCIDS), AISSIM 200, and/or the National Industrial Security Program Operations Manual (NISPO) and Supplement hereby incorporated by reference and made a part thereof (as appropriate). "Reference Item 10e(2): This contractor will follow the requirements of DCID 6/5 Policy for the Protection of Certain non-SCI Sources and Methods Information (SAMI) and DCID 6/6 Security Controls on the Dissemination of Intelligence Information." Reference Item 10j: Guidance for FOUO may be found in the NSM, paragraph 11-705. Any and all security policy changes to or revisions of the documents outlined above will be distributed to the contractor by the contracting officer and will become added requirements to this contract. Security requirements are a material condition of this contract. Failure of the contractor to maintain and administer a security program, fully compliant with the security requirements of this contract, constitutes grounds for termination for default.

If, subsequent to the date of this contract, the security requirements under this contract are changed by the Government, as provided in this clause, and the security costs or time required for delivery under this contract are thereby increased or decreased, the contract price, delivery schedule, or both, and any other provision of this contract which may be affected shall be subject to an equitable adjustment. Any equitable adjustment required by virtue of this clause shall be accomplished in the same manner as equitable adjustment negotiate under the Changes clause of this contract.

See attached

14. ADDITIONAL SECURITY REQUIREMENTS. Requirements, in addition to ISM requirements, are established for this contract. ☐ Yes ☒ No
(*If Yes, identify the pertinent contractual clauses in the contract document itself, or provide an appropriate statement which identifies the additional requirements. Provide a copy of the requirements to the cognizant security office. Use Item 13 if additional space is needed.*)

15. INSPECTIONS. Elements of this contract are outside the inspection responsibility of the cognizant security office. ☐ Yes ☒ No
(*If Yes, explain and identify specific areas or elements carved out and the activity responsible for inspections. Use Item 13 if additional space is needed.*)

16. CERTIFICATION AND SIGNATURE. Security requirements stated herein are complete and adequate for safeguarding the classified information to be released or generated under this classified effort. All questions shall be referred to the official named below.

a. Typed Name of Certifying Officer Rosalind Schlink	b. Title Chief of Security	c. Telephone (<i>Include Area Code</i>) 571-432-1362
d. Address (<i>Include Zip Code</i>) same as 6c. above	17. REQUIRED DISTRIBUTION <input checked="" type="checkbox"/> a. Contractor <input type="checkbox"/> b. Subcontractor <input checked="" type="checkbox"/> c. Cognizant Security Office for Prime and Subcontractor <input type="checkbox"/> d. U.S. Activity Responsible for Overseas Security Administration <input type="checkbox"/> e. Administrative Contracting Officer <input type="checkbox"/> f. Others as Necessary:	
e. Signature		

"Reference Item 11c: Contractor requires access to classified source data up to and including "TOP SECRET//SI//TK" in support of the work effort. Any classified information or extracts generated in the performance of this contract requires the contractor to apply derivative classifications and markings consistent with the source documents. Use of "Multiple Sources" on the "DRV FROM" line necessitates the inclusion of a listing of the specific source classification guides."

The contractor may be required to prepare a System Security Plan (SSP) and any other applicable documents depending on the established Protection Level for their Information System (IS) and the system will require approval of the CSO/DAA in accordance with DCID 6/3 Industry Overprint. The contractor will be required to adhere to the requirements applicable to Information Technology (IT) outlined in the NSM, DCID 6/3 and the DCID 6/3 Industrial Overprint, the NRO C&A Process for Information Systems as well as any updates or supersessions to these documents." The contractor agrees to permit the necessary polygraph interviews of contractor personnel requiring access to such information. It is understood that the polygraph interview will be limited to counter-intelligence issues.

The prime contractor is responsible for providing security oversight and ensuring an effective security program for any and all subcontractor relationships that are formed as the result of the contract. The contractor shall obtain pre-contract approval from the Contracting Officer of any subcontractor relationship where the disclosure of classified information to that subcontractor is necessary in order to accomplish the purposes of the contract. If it becomes necessary to disclose classified information in a subcontract relationship not previously approved in accordance with the above, the contractor shall request permission of the Contracting Officer prior to such disclosures. The request shall be in writing and shall identify the specific subcontractor and the nature and extent of classified information which needs to be disclosed. The contractor is expressly prohibited from representing subcontractor's employees as prime contractor's employees for the purpose of obtaining access to classified materials for these individuals. Requests for such access shall specifically identify the company for whom each employee works. The contractor agrees to include in all such subcontracts provisions which shall conform substantially to the language above and such other paragraphs as the Contracting Officer may direct.

Whenever the contractor, in performance of the work under this contract, finds that the requirements of any of the clauses are in conflict with security instructions issued by the Contracting Officer or by a duly authorized representative for security matters, the contractor shall call the attention of the Contracting Officer to such conflict. The Contracting Officer or his duly authorized representative for security matters shall: (1) Modify or rescind such security requirements, or (2) The Contracting Officer shall issue to the contractor written instructions concerning compliance with the requirements of the clauses or provisions conflicting with such security requirements. Any waiver of compliance with the clauses or provisions of this contract issued by the Contracting Officer shall be in writing. In the event a conflict occurs between the various security manuals, the contractor will utilize the most restrictive guidance and immediately refer the matter to the cognizant program security officer for resolution. In the event that the development of information or material is not clearly covered by the contract or regulations, the contractor is required to seek Government guidance regarding its handling.

"Reference Item 11g:

*a. The contractor must prepare and forward DD Forms 1540 and 1541 to the CO for authorization **BEFORE** the services may be requested.*

b. Technical information on file at the Defense Technical Information Center (DTIC) will be made available to the contractor if the contractor requires such information. The contracting officer will certify the field of interest relating to the contract.

The Contractor will coordinate the use of other US Government couriers with the PSO.

The contractor shall maintain all modified and/or fabricated hardware at the proper classification level (s) and environment (s).

It is a material condition of this contract that the contractor shall not use, or allow to be used, any aspect of this contract for publicity, advertisement, reference or any other public purposes without specific approval. The contractor may request a waiver or release from the non-publicity clause (see clause language in contract), but shall not deviate from it unless authorized to do so in writing by the contracting officer. However, for those companies who have been specifically authorized in writing *either outside the scope of this acquisition or as the result of unclassified association on this specific acquisition*, the following unclassified information may be published as determined by company policy/corporate personnel since this statement is not considered an aspect of the contract per current clause language: "(Company) provides support to the National Reconnaissance Office (NRO), the US Government agency responsible for operating US reconnaissance satellites." (actual verbiage should be obtained from the Office of Contracts letter sent to the company advising them of declassified association, if applicable)

Contractor personnel directly supporting this contract may also be permitted to acknowledge their contract in support of the NRO for business purposes with prior guidance from the appropriate PSO as long as the contract prefix begins with "NRO". Acknowledgement must not result in publication and will depend on the activities proscribed by the contract. However, contractor personnel will not acknowledge such contract support or affiliation when traveling to sensitive operational locations or classified sites.

Unless prior written approval is obtained from the contracting officer, the contractor is prohibited from using any aspect of this contract for publicity, advertisement, reference, or any other public purposes. Prior written approval will be required even when disclosure is required by a federal statute or regulation, e.g., Securities Exchange Commission filings, past performance reporting, etc. A request for a waiver that includes a copy of all such intended filings or disclosures shall be promptly forwarded to the contracting officer prior to any public release.

Operations Security (OPSEC) requirements of the contract may require the identification, separation, and protection of project data and the use of OPSEC for some or all aspects of the program.

Technology related to this contract and funded by the NRO must be submitted to the Program Security Office for evaluation and determination of appropriate security classification and control. This determination must be completed prior to any dissemination of information on the program.

PRIVACY OR SECURITY SAFEGUARDS (MAR 1996)

(a) The detail of any safeguards the contractor may design or develop under this contract are the property of the Government and shall not be published or disclosed in any manner without the contracting officer's express written consent.

(b) The details of any safeguards that may be revealed to the contractor by the Government in the course of performance under this contract shall not be published or disclosed in any manner without the contracting officer's express written consent.

(c) The Government shall be afforded full, free, and uninhibited access to all facilities, installations, technical capabilities, operations, documentation, records, and data bases for the purpose of carrying out a program of inspection to ensure continued efficacy and efficiency of safeguards against threats and hazards to data security, integrity, and confidentiality.

(d) If new or unanticipated threats or hazards are discovered by either the Government or the contractor, or if existing safeguards has ceased to function, the discoverer shall immediately bring the situation to the attention of the other party. Mutual agreement shall then be reached on changes or corrections to existing safeguards or institution of new safeguards, with final determination of appropriateness being made by the Government. The Government's liability is limited to an equitable adjustment of cost for such changes or corrections, and the Government shall not be liable for claims of loss of business, damage to reputation, or damages of any other kind arising from discovery of new or unanticipated threats or hazards, or any public or private disclosure thereof.

TELECOMMUNICATIONS SECURITY EQUIPMENT, DEVICES, TECHNIQUES, AND SERVICES (MAR 1996)

(a) Definitions. As used in this clause:

(1) "Securing" means the application of Government-approved telecommunications security equipment, devices, techniques, or services to contractor telecommunications systems.

(2) "Sensitive information" means any information the loss, misuse, or modification of which, or unauthorized access to, could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under 5 U.S.C. 552a (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or Act of Congress to be kept secret in the interest of national defense or foreign policy.

(3) "Telecommunications systems" means voice, record, and data communications, including management information systems and local data networks that connect to external transmission media, when employed by Government agencies, contractors, and subcontractors to transmit:

(i) Classified or sensitive information;

(ii) Matters involving intelligence activities, cryptologic activities related to national security, the command and control of military forces, or equipment that is an integral part of a weapon or weapons system; or

(iii) Matters critical to the direct fulfillment of military or intelligence missions.

(4) Communications Security (COMSEC) Information: A COMSEC account shall be acquired through the local Regional COMSEC Office (RCO). The contractor shall meet all requirements for briefing, indoctrination, handling, and inspection as outlined in the most current version of the COMSEC Security Manual. The Contractor Facility Security Officer, will submit to the RCO names of individuals for approval for access to COMSEC controlled information or material. *"Reference Item 10a: NAM CLAUSE N52.204-004 applies."*

(b) This solicitation/contract identifies classified or sensitive information that requires use of secure telecommunications by the Contractor. The Contractor agrees to secure information and systems at the following locations as identified in Item 8: (c) To provide the secure connectivity, the Contractor shall work with the regional NRO COMSEC Office to identify requirements, equipment, and coordinate installation of GFE and CFE.

(c) The Contractor agrees to include this clause, including this paragraph (d), in all subcontracts which require COMSEC (e) The contractor agrees to include this clause, including this paragraph (e), in all subcontracts which require securing telecommunications.

UNESCORTED ACCESS

Contractor personnel requiring unescorted access to Government facilities shall be required to meet DCID 6/9 security standards. The contractor shall include the substance of this requirement in all subcontracts in which subcontractor personnel will require unescorted access to Government facilities. Contract performance is restricted to NSSO, 11242 Waples Mill Road, Fairfax, 14675 Lee Road, Suite 14A00, 1670 , Air Force Pentagon, Suite 4C1000, Washington DC, mission partner locations, and General Dynamics company locations. Using contractor or government activity will provide security classification guidance for performance of the contract.

Contractor requires access to classified source data up to and including (TOP SECRET, SECRET, or CONFIDENTIAL -- insert one) in support of the work effort. Any classified information or extracts generated in the performance of this contract requires the contractor to apply derivative classifications and marking consistent with the source documents. Use of "Multiple Sources" on the "classified by" line necessitates the inclusion of a listing of the specific source classification guides.

N52.204-005 Protection Against Compromising Emanations

PROTECTION AGAINST COMPROMISING EMANATIONS (MAR 1996)

(a) The Contractor shall provide/use equipment to process national security information that meets the emanations accreditation profile of the SCIF as determined by a TEMPEST review in accordance with the National Telecommunications and Information Systems Security Policy (NSTISSP No. 300, National Policy on Control of Compromising Emanations (C)) and Instruction No. 7000 [NSTISSI 7000. TEMPEST Countermeasures for Facilities (C)].

(Requirement for spacecraft or any systems using transmitters should incorporate the following.)

(b) Equipment, systems, and facilities that process national security information and which present the potential to exhibit NONSTOP emanations shall conform to National Security Telecommunications and Information Systems Security Instruction (NSTISSI) No. 7001, "NONSTOP Countermeasures," and applicable portions of NACSEM 5112, NONSTOP Evaluation Techniques.

Requirements for contract deliverables that process classified information. (There are no TEMPEST requirements on equipment per se.)

(c) Contract deliverables that process national security information shall be designed to minimize the possibility of compromising emanations.

(d) The Government may, as part of its inspection and acceptance, conduct additional tests to ensure that equipment or systems delivered under this contract satisfy the security standards specified. The Government may conduct additional tests:

(1) At the installation site or contractor's facility.

(2) Notwithstanding the existence of valid accreditations of equipment prior to the award of this contract.